Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:38:45 UTC

Tool: ChChes

Names	ChChes HAYMAKER Ham Backdoor Scorpion
Category	Malware
Type	Backdoor
Description	(Palo Alto) In addition to using PlugX and Poison Ivy (PIVY), both known to be used by the group, they also used a new Trojan called “ChChes” by the Japan Computer Emergency Response Team Coordination Center (JPCERT). In contrast to PlugX and PIVY, which are used by multiple campaigns, ChChes appears to be unique to this group. An analysis of the malware family can be found later in this blog. Interestingly, the ChChes samples we observed were digitally signed using a certificate originally used by HackingTeam and later part of the data leaked when they were themselves hacked. Wapack labs also observed a similar sample targeting Japan in November. It’s not clear why the attackers chose to use this certificate, as it was old, had been leaked online, and had already been revoked by the time they used it. Digital certificates are typically used because they afford an air of legitimacy, which this one definitely does not.
Information	<https://unit42.paloaltonetworks.com/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/> <https://www.cylance.com/en_us/blog/the-deception-project-a-new-japanese-centric-threat.html> <https://www.jpcert.or.jp/magazine/acreport-ChChes_ps1.html> <https://www.jpcert.or.jp/magazine/acreport-ChChes.html> <https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0144/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.chches>

AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:chches>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool ChChes

Changed	Name	Country	Observed	
APT groups				
	Snake Wine		2016	
	Stone Panda, APT 10, menuPass		2006-Mar 2025	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=641359e0-3415-45b2-a304-860ecb58ac7d